148

Abstract of the Disclosure

In a database, a frequently retrieved column is encrypted using a common key, and other columns are encrypted using a specific row key. Thus, a retrieving process can be performed at a high speed, and the security can be improved. Then, the row and column of the database are encrypted by assuming the plaintext to be encrypted as a bit string, and performing a binary operation with a random bit string. A random bit string is obtained by sequentially generating multidimensional vectors using a nonlinear function by defining a predetermined bit length as 1 word and a plurality of words as components of the multidimensional vector.